Approving University Officials: Provost, Senior Vice President for Business and Finance
Responsible Office: NUIT Information Security Office
Effective Date: September 1, 2019
Next review Date: September 1, 2020

APPROPRIATE USE OF ELECTRONIC RESOURCES

Policy Statement

The University is committed to ensuring open discourse and the free expression of viewpoints and beliefs. This commitment includes ensuring that academic dialogue is free from unwarranted institutional intrusion and oversight. With the values of open discourse and institutional restraint as guideposts, the purpose of this University-wide policy is to articulate and promote the ethical, legal, and secure use of information technology by all members of the Northwestern community and to confirm the University's responsibilities in connection with accessing such information. This policy establishes essential guidelines, protocols, and standards of behavior for the use of Electronic Resources at Northwestern. It applies to all (i) computing and networking equipment owned, leased, or operated by Northwestern; (ii) software owned, leased, operated, or contracted by Northwestern or for use for Northwestern business; and (iii) other devices where University Information is present, regardless of ownership.

For purposes of this policy, the terms Electronic Resources, University Information, and System User have the meanings defined below.

Purpose

Northwestern makes available Electronic Resources to community members so that they can share and store knowledge, communicate, and conduct business in support of the University's mission. The University is committed to maintaining an environment in which academic freedom thrives. At the same time, the University needs to ensure the security and stability of the Electronic Resources it makes available to community members. This policy identifies the general circumstances under which University Information may be accessed or disclosed. Approval for access to a System User's information is guided by the following six principles:

- Access should occur only for a legitimate University purpose.
- Access should be authorized only by appropriate and accountable people.
- Notice of access should be given to affected System Users, except in cases where access cannot be disclosed for legal or investigatory purposes or when access is incidental to routine IT procedures in support of University network and computing resources.
- Access should be limited to the University Information needed to accomplish the purpose.
- Sufficient records should be kept to enable appropriate review of compliance with this policy.
- The Policy Review Committee should evaluate the policy and anonymized reports regarding access on a periodic basis.

Audience

Any individual using Electronic Resources, including but not limited to faculty, staff, undergraduate and graduate students, postdoctoral trainees, retirees, researchers, alumni, contractors, vendors, volunteers, and visitors.

Definitions

Electronic Resources: computing and telecommunications devices and systems that can execute programs or access, store, or transmit University Information. Examples of Electronic Resources may include but are not limited to computers, servers, networks, mobile computing devices, smartphones, storage devices (USB or otherwise connected); software owned, leased, operated, or contracted by Northwestern or for use for Northwestern business; email; and personally-owned resources used for University business.

System User: any individual accessing Electronic Resources.

University Information: any data, information, or business records created, processed, or stored on, transmitted through, or otherwise traversing the University network.

Policy Implementation

1. ***Privacy/Confidentiality***

1.1. Northwestern's Electronic Resources are intended primarily for the execution of University business. Northwestern strives to ensure the integrity of individual and institutional information stored in its systems. The University reserves the right to examine, capture, archive, and otherwise preserve or inspect any data or information related to Electronic Resources that is either transferred over University networks or systems, created or stored on University-owned equipment, or created or stored on personally-owned resources when used for University business.

1.2. Northwestern community members with access to Electronic Resources are expected to respect the privacy of the individuals whose information they access and to use reasonable and prudent methods to preserve the integrity and privacy of the accessed information to the extent possible. Community members with access to Electronic Resources are prohibited from using or disclosing that information for any purpose except in the course of University business with those who have a need to know, and they shall take necessary precautions to protect the confidentiality of personal information. Specific standards containing Information Privacy and Security requirements are located on NUIT's Information Security Office website.

1.3. Although the University does not routinely monitor the information content exchanged or stored on its systems, users should be aware that the University retains the right to access Electronic Resources when necessary and appropriate in light of the six principles mentioned above in the Purpose section. The content of user files, electronic mail, and network transmissions will not be viewed, monitored, altered, or disclosed except where:

1.3.1. required by law, regulation, policy, rule, court order, or subpoena;

1.3.2. required for a governmental, civil, and/or criminal investigation;

1.3.3. there is a well-defined and documented University mission-related need for information, including, but not limited to: (a) conducting University investigations of alleged violations of law, policy, academic dishonesty or research integrity; (b) conducting internal audits; or (c) where such information is necessary to meet the university's teaching, research, administrative and/or compliance obligations and where such access is limited to the information needed to accomplish the purpose.

1.3.4. there is a credible allegation or actual evidence of a violation of University policy and/or state or federal law; or

1.3.5. IT procedures in support of University network and computing resources result in incidental exposure to file details and content. IT personnel will not intentionally access, review, or disclose file details or contents not related to such support procedures.

1.4. The University will notify System Users when it is necessary to access Electronic Resources, except for IT procedures in support of University network and computing resources or in limited circumstances where it is prohibited by law, regulation, subpoena, or where notification would impede an investigation. Personnel requesting access to Electronic Resources will be responsible for notifying System Users.

1.5. Approval for access to Electronic Resources and information must be obtained and documented as follows, except for IT procedures in support of University network and computing resources or where the government or other authority does not allow for such disclosure:

1.5.1. *Academic Appointees*: approval must come from designees in the Office of the Provost and the Office of General Counsel

1.5.2. *Staff (except postdoctoral trainees)*: approval must come from designees in the Office of Human Resources and the Office of General Counsel

1.5.3. *Postdoctoral trainees*: approval must come from designees in the Office of Human Resources (in consultation with the Graduate School, where necessary) and the Office of General Counsel

1.5.4. *Graduate Students*: approval must come from designees in the Graduate School and the Office of General Counsel

1.5.5. *Undergraduate Students*: approval must come from designees in the Student Affairs Division and the Office of General Counsel

1.5.6. *Alumni*: approval must come from designees in the Alumni Relations and Development and the Office of General Counsel

1.5.7. *All Others*: approval must come from designees in the Office of General Counsel

Approval for access to a System User's information is guided by the six principles mentioned in the Purpose section.

The Office of General Counsel Will be responsible for retaining the requests and approvals pursuant to the University's Record Retention Policy.

2. ***Personal Usage Policy***

2.1. Northwestern provides Electronic Resources to enable individuals with academic, research, and administrative appointments and students in good standing to accomplish work that serves the mission of the University. Upon request, alumni are provided access to University email for personal use.

The University will consider community members' rights to free expression and academic freedom when determining whether personal use of Electronic Resources is permissible.

2.2. Incidental personal use of Electronic Resources is permitted, so long as the use:

2.2.1. does not adversely affect the performance of the individual's official duties or the University's work;

2.2.2. is not disruptive to and does not adversely affect others;

2.2.3. does not create a conflict of interest or commitment for the individual or the University; and

2.2.4. does not constitute illegal or prohibited activity, including the prohibited activities referenced in Section 3 below.

3. ***Prohibited Activities***

Northwestern welcomes the expression of ideas, including viewpoints that may be considered unorthodox or unpopular. However, community members may not violate any laws or University policies through the use of Electronic Resources. In particular, community members are prohibited from engaging in the activities described below. The University will consider community members' rights to free expression and academic freedom when investigating reports of suspected prohibited activity.

3.1 *Unauthorized Access.* Individuals with authorized access to University systems may not intentionally provide information or access to technology resources to anyone who is not authorized, seek information for which they are not authorized, assist others in doing so, attempt to subvert or circumvent any University systems' security measures (e.g. sharing passwords), or use Electronic Resources to subvert or circumvent any other systems' security measures for any purpose.

3.2 *Obstructing Access or Damaging Resources.* System Users may not engage in any activity that intentionally disrupts or damages software, hardware, or other resources belonging to the University or compromise the ability of others to use such resources.

3.3 *Inappropriate Use.* System Users may not use Electronic Resources to engage in copying or distribution of software or digital content; phishing; circulating spam; etc. that violates the law or terms of a University license agreement.

3.4 *Violation of Law or Other Northwestern Policies.* System Users may not use Northwestern Electronic Resources in a manner that violates the law or other University policies, including but not limited to policies on Minors at Northwestern, Sexual Misconduct, Discrimination and Harassment, and Civility and Mutual Respect.

4. ***Reporting; Protection against Retaliation***

Any community member who has observed, has knowledge of, or has been the victim of any improper or prohibited use of Northwestern's Electronic Resources is encouraged to report such activity by contacting the NUIT Information Security Office (see "Contacts" below for additional information).

Northwestern community members who prefer to report anonymously may do so by utilizing EthicsPoint, the University's phone- and web-based system for confidential reporting of suspected misconduct.

The University's Policy on Non-Retaliation prohibits retaliation against any member of the Northwestern community for acting, in good faith, to report suspected improper or prohibited use of Electronic Resources, to assist another in reporting, or to participate in the investigation of a report.

Consequences of Violating this Policy

Administrators of Northwestern's Electronic Resources may restrict or refuse access privileges to individuals who violate this policy.

Individuals who are found to have engaged in prohibited activities under this policy may be subject to discipline under University policies and procedures (including the code of conduct and handbooks referenced below), up to and including termination of employment or academic dismissal. Additionally, the University may contact the appropriate governmental authority when notified of suspected violations of federal, state, or local laws or regulations.

Related Information

University Policies

Civility and Mutual Respect

Discrimination and Harassment

Minors at Northwestern

Non-Retaliation

Sexual Misconduct

Other Information

EthicsPoint

Northwestern Faculty Handbook

Northwestern Staff Handbook

Northwestern Student Handbook

NUIT Information Security Office website

Contacts

The following office can address questions regarding this Policy:

Information Security Office, NUIT
(847) 467-4741;
security@northwestern.edu

To report violations of this policy or other improper use of Northwestern's Electronic Resources, contact the NUIT Information Security Office at the phone number or email address listed above, or call (847) 491-HELP (4357).

The following individuals can address questions regarding approvals for access:

Name	***Office***	***Contact Information***
Andrea Bueschel	Office of the Provost	(847) 491-6699 bueschel@northwestern.edu
Stephanie Griffin	Human Resources	(847) 467-0438 stephanie.griffin@northwestern.edu
Julie Payne-Kirchmeier	Student Affairs	(847) 467-2779 jp-kirchmeier@northwestern.edu
Karyn Reif	Alumni Relations	(847) 467-7129 karyn.reif@northwestern.edu
Sergey Kucherenko	The Graduate School	sergey.kucherenko@northwestern.edu
Priya Harjani	Office of General Counsel	(847) 491-5573 p-harjani@northwestern.edu

History

New policy effective **September 1, 2019.**

This policy supersedes the following University Policies:

- Privacy within the Northwestern Network (originally issued in December 2002 and revised in 2003 and 2012).
- Prohibited Use of Electronic Resources for Threats, Harassment, and Pornography (originally issued in June 2010).
- Rights and Responsibilities for the Use of Central Network and Computing Resources (originally issued in June 2003 and revised in 2008 and 2012).

Policy URL:

https://policies.northwestern.edu/docs/appropriate-use-policy-final.pdf